#10
8/30/03
ymel

Docket No.: 080398.P245

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Brant L. Candelore	Examiner: John Weiss
Application No.: 09/430,043	Art Group: 3629
Filed: October 29, 1999	
For: Copy-Protecting Management Using a User Scrambling Key	

DECLARATION UNDER 37 CFR §1.131

Assistant Commissioner for Patents
Washington, DC 20231-9998

Sir:

I, Brant L. Candelore, declare that:

1. I am the sole inventor of the subject matter claimed in the above-identified patent application.

2. This declaration is to establish conception of the invention in this application in the United States, at a date prior to April 7, 1999, which may be considered by the Examiner as the earliest effective filing date of U.S. Patent No. 6,314,425B1 issued to Serbinis, et al.

3. I understand that the invention relates to the following:

A. A method to provide copy protection for a content, the method comprising:

receiving an authorization code via a communication channel, the communication channel being one of a return path of a cable connection, a telephone connection, and a network;

generating a local key from a programmable user key according to an authorization code provided by a content provider; and

descrambling the content delivered by the content provider using a local key

B. A conditional access (CA) device comprising:

a descrambler to descramble a content delivered by a content provider using a local key;

a key generator coupled to the descrambler to generate the local key from a user key according to an authorization code provided by the content provider; and

a communication interface coupled to the key generator to receive the authorization code via a communication channel, the communication channel being one of a return path of a cable connection, a telephone connection, and a network

C. A computer program product comprising:

a computer usable medium having computer program code embodied therein to provide copy protection for a scrambled content, the computer program product having:

a first program code to descramble the content delivered by a content provider using a local key;

a second program code to generate the local key from a programmable user key according to an authorization code provided by the content provider; and

a third program code to receive the authorization code via a communication channel, the communication channel being one of a return path of a cable connection, a telephone connection, and a network.

4. Prior to April 7, 1999, I completed an invention disclosure (Exhibit A) describing the invention and submitted the invention disclosure to the legal department of Sony Electronics, my employer.

5. After receipt of the invention disclosure, the legal department of Sony Electronics requested Blakely Sokoloff Taylor & Zafman, LLP to prepare and file a patent application on the subject matter set forth in Exhibit A.

6. Thereafter, the above-identified patent application was prepared with due diligence and filed on October 29, 1999.

I hereby declare that all statements made herein of my own knowledge are true and that the statements made on information and belief are believed to be true and, further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: 7/9/03

Brant L. Candelore

Appendix A

INVENTION DISCLOSURE FORM

I. IDENTIFICATION IPD Case #: _____

1. Short Descriptive Title of the Invention:

Method for Copy-Protecting Content by Using a User Scrambling Key

2. Name of Responsible Patent Coordinator (if any):

N/A

3. Identify all persons who contributed to the present invention including persons from other Sony Divisions, Sony Japan and Outside Companies. Final determination of inventorship is a legal question which will be resolved at a later time.

(1) Full Legal Name: Brant L. Candelore
Home Address: [redacted]

Citizenship: U.S.A.
Business Phone/Fax: [redacted]
Division/Company/Location: DNSA
Manager's Name / Phone No.: [redacted]

(2) Full Legal Name:
Home Address:

Citizenship:
Business Phone/Fax
Division/Company/Location
Manager's Name / Phone No.

(Add names as necessary)

II. BACKGROUND INFORMATION

1. Do you believe this invention was developed while working under or in the performance of experimental, developmental or research work called for by a Government Contract or upon the understanding that a Government Contract would be awarded? [X]NO [ ]YES

2. Has your invention been disclosed to anyone outside of Sony in a speech, exhibit, presentation, product, product manual, report, lecture, trade show, technical article, publication or otherwise? [X]NO [ ]YES

3. Is this invention related to any previous Sony Invention Disclosures of which you are aware (made by you or someone else)? [ ]NO [X]YES

[redacted]

4. If you responded "YES" to any of questions 1-3, please explain below:

5. Name of product(s) or project(s) for which this invention was developed: **Electronic Media Distribution**

6. When do you expect a product incorporating this invention to be sold, offered for sale or shown to someone outside of Sony? (If a product or prototype has already been sold, offered for sale or shown, please identify the earliest date this happened.): **UNKNOWN**

7. Has a working model of the invention been built and tested (or appropriate software been written)?
[X]NO [ ]YES If yes, who has witnessed a demonstration, and when?

8. List below any patents, publications, articles, texts, products, etc. which describe technology similar to your invention including reference material which may be useful in understanding the background technology of your invention: Include a copy of each item to IPD. Please include copies of all bibliographical information.)

Signature of Submitter(s):_____ **Date:** _____

Read and understood by: _____ **Date:** _____

III. DESCRIPTION OF THE INVENTION

Provide a complete technical description of your invention including the following items where possible. You may attach documentation in the form of letters, memos, engineering notebook pages, etc. if available, or you may use as many invention disclosure data sheets as necessary. Be sure each page is signed, dated and witnessed.

1. **Explain the problems, issues or needs which led to the invention, and explain how others have addressed these problems, issues or needs?**

Basic Terminology

ACCESS CONROL - Algorithms running in a "secure" processor used to determine whether or not a decoder is authorized to view a particular program. The program may be given away (and therefore unscrambled or in-the-clear), needing a subscription, or needing the user to make a purchase.

CONDITIONAL ACCESS – Same as Access Control.

EMM - Entitlement Management Message. A message used to deliver privileges to a set-top box. The EMM message delivers rights and keys. The encrypted key delivered is usually a function of the rights granted, hence a modification of the rights by a pirate means the delivery of a bad key.

ECM - Entitlement Control Message. Message which regulates access to a particular channel. It determines which access right needs to be held by the decoder in order to grant access. The ECM is used to either deliver the key used to scramble content or information to derive that key.

IPPV - Impulse Pay Per View - Feature which allows purchases of pay-per-view movies through credit that has been previously downloaded into the set-top box. Purchase records are stored and forwarded by phone to billing center.

Background:

The field of the invention relates to the storing of scrambled content, and the problems associated with replaying that content back to a Conditional Access (CA) device days, months and even years later.

The invention pertains to processing that is done to control messages or scrambling of digital content for storage to media for later retrieval.

PRIOR ART

Current CA Devices typically use Unique Keys to deliver a Group Key in EMM messages. Typically the "Group" are customers that share a particular set of entitlements. Unit Keys are typically not used to descramble content because content usually broadcast to more than one device.

Problem #1: If Content is locally scrambled with Unique CA Keys, then it is difficult to playback to CA devices located elsewhere, e.g. Car, Bedroom, 2nd Home.

Problem #2: If CA device which was used to locally scramble content fails (quits working), then the content stored with that device may not be retrievable.

The invention solves this and other problems.

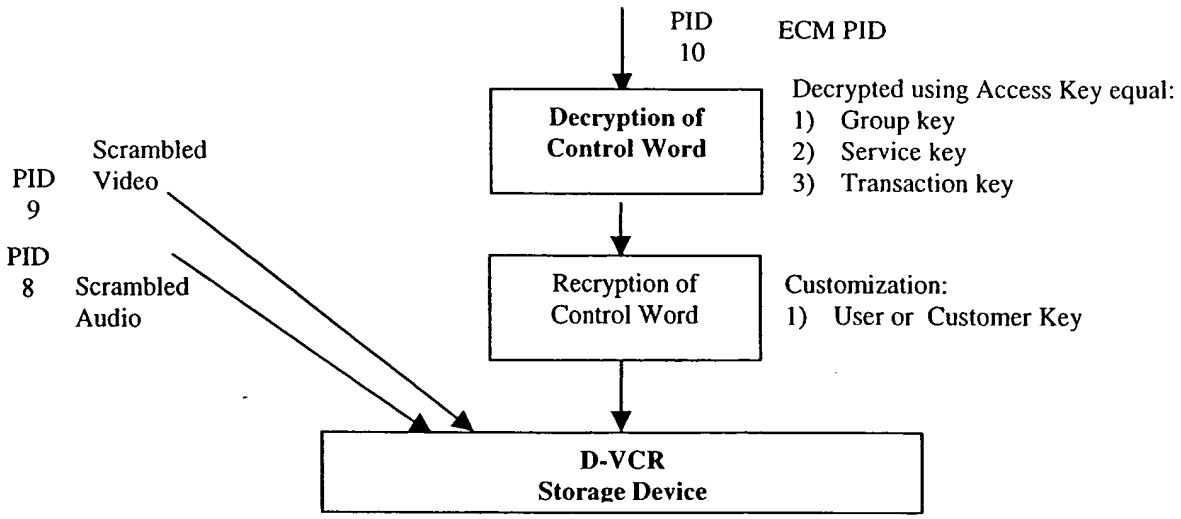
2. **Best Mode: Describe any and all preferences you personally have regarding how to best implement, build, produce, or use your invention (e.g. preferred parts, materials, techniques, etc. which you feel are best in practicing your invention). Each submitter's opinion is important here, even if there is disagreement. Please list anything you think will make the invention better in any way.**

Invention #1: Use of a static USER KEY which may be downloaded to each CA device, may be used to access content by multiple CA devices sharing that same key.

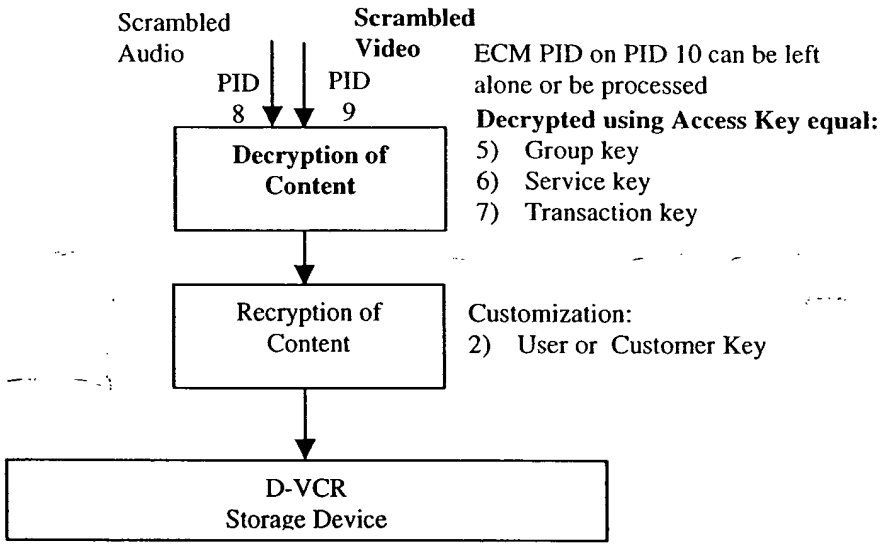
If content is to be User Encrypted, to make a personal copy and not one for sharing, then the CA device may use a special User Key. The Key is unique for the customer or perhaps the customer's immediate or extended family. The User Key may be downloaded to all CA devices the customer may have under his control. If a particular CA device fails, it does not matter because the same User Key may be downloaded to a new CA device. The User Key is used to enforce Copy Protection of content that was delivered over a network when it is not "Copy Free".

A Content Provider may wish to release content as Personal Copies and not ones that may be easily shared. The content may be sent from the Content Provider already encrypted under the User Key. Or the content may be re-scrambled locally under the User Key, e.g. after PPV operation is made.

Decryption and Re-encryption of Control Words



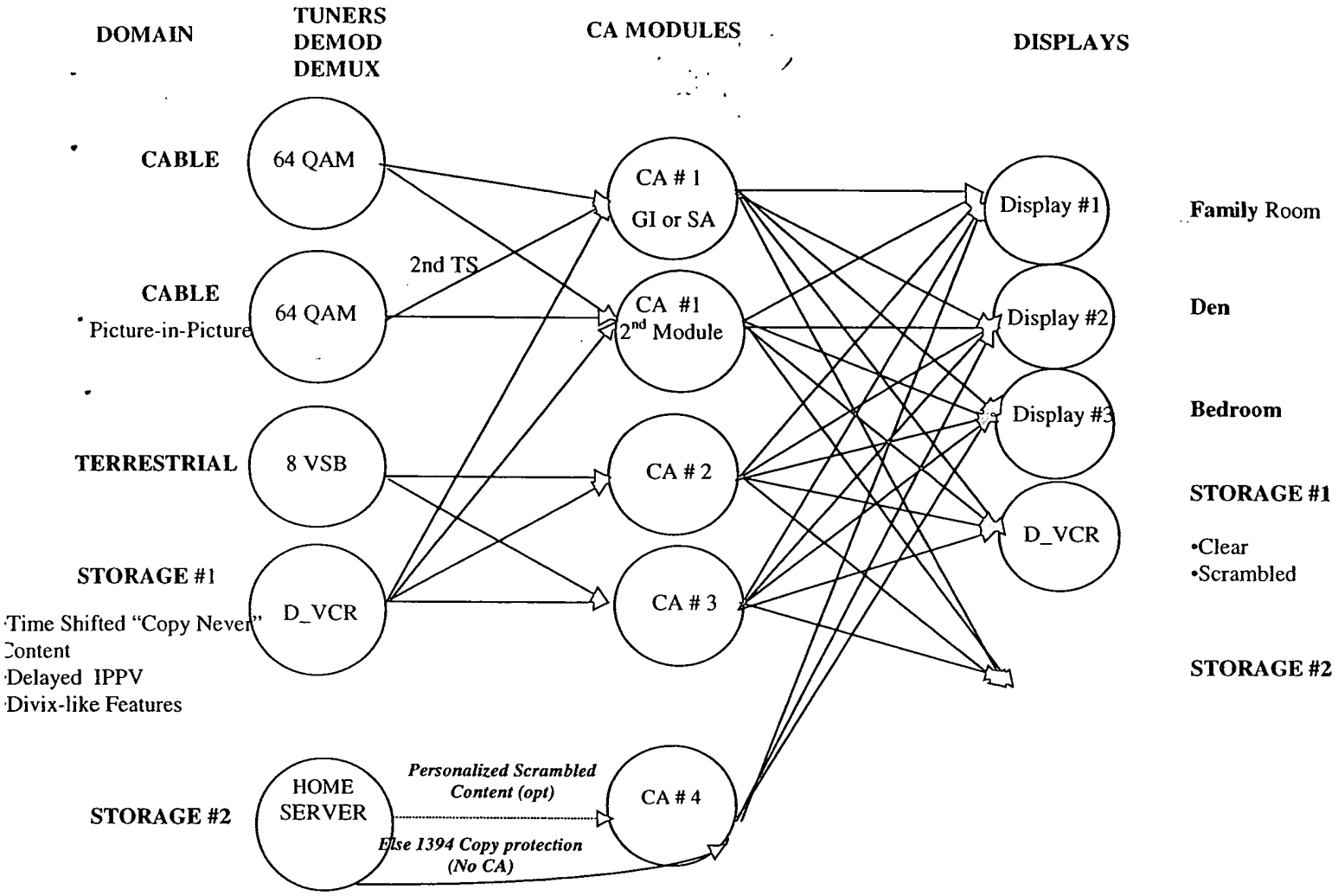
Decryption and Re-encryption of Content



3. Briefly describe any alternate uses, variations or modifications of your invention which you contemplate.

The User Key may have other access parameters, e.g. time or per-play, etc. ...

4. Describe the construction and operation of the invention including drawings (flow charts, schematics, block diagrams, mechanical drawings, photographs, etc.).



Invention Disclosure Data Sheet

Signature of Submitter(s):_____ **Date:** _____

Read and understood by: _____ **Date:** _____